[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 9/08
G07C 9/00

[12] 发明专利申请公开说明书

[21] 申请号 95194945.4

[43]公开日 1997 年 8 月 20 日

[11] 公开号 CN 1157677A

[22]申请日 95.9.6

[30]优先权

[32]94.9.7 [33]US[31]08/301,677

[32]95.8.8 [33]US[31]08/512,491

[86]国际申请 PCT/CA95/00509 95.9.6

[87]国际公布 WO96/08093 英 96.3.14

[85]进入国家阶段日期 97.3.7

[71]申请人 米泰克技术有限公司

地址 加拿大安大略

[72]发明人 乔治·J·托莫克 克林·苏塔格里高利·J·施密特

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

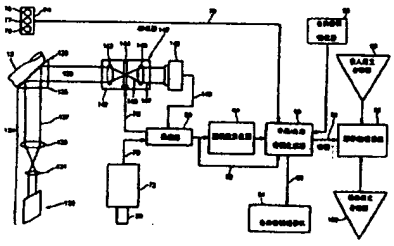
代理人 鄂 迅

权利要求书 4 页 说明书 13 页 附图页数 4 页

[54]发明名称 由生物统计控制的密钥生成

[57]摘要

按如下实现一种密钥生成系统。通过对用户指纹信息的处理在登记设备上生成一个唯一数。接着产生一个滤波器，它是用户指纹的傅里叶变换和该唯一数的函数。在用户卡上存储该滤波器。用户把卡放入一个设备的读卡器里并把他的手指按在指纹输入器上。该设备从指纹输入中生成光傅里叶变换，信号入射到一个用该卡的滤波器信息编程的空间光调制器上。从滤波后的信号生成逆变换，并用该逆变换生成密钥。



一个用户可能使用图 2 的设备 70 传递他的公共密钥或者解密报文。此外，另一个用户可能利用设备 70 加密报文。

现转向图 2，设备 70 包括一个输入系统 129，该输入系统带有一个激光器 130、放大透镜 131、准直透镜 133 和棱镜 135，它可类似于图 1 的输入系统 29。相关器 142 位于信息束通路 139 中。该相关器包括一个傅里叶变换透镜 143、一个位于透镜 143 的后焦面里的电子可寻址（可编程）空间光调制器（SLM）144 以及一个逆傅里叶变换透镜 146。从相关器输出的光束 147 输入到光检测器 148。光检测器输入给线路 149 上的处理器 80。该处理器还在线路 78 上接收来自读卡器 72 的输入。该处理器输出到线路 79 上的 SLM144、伪随机数发生器 84 以及线路 82 上的公共/专用密钥生成器。伪随机数发生器向公共/专用密钥生成器输出，该密钥生成器又输出到公共密钥通信机 94 以及线路 92 上的解密/加密系统 96。公共/专用密钥生成器还从公共密钥接收机 95 以及辅助键盘 74 接收输入。解密/加密系统从输入报文存储器 98 接收输入并向输出报文存储器 100 输出。

希望传送自己的公共密钥的用户如在登记期间把手指按在屏 28（图 1）上一样把相同的手指按在输入屏 128 上，把他的卡 20 放入到读卡器 72 里并且按动辅助键盘 74 的按钮 76。这激活光源 130 并且来自棱镜的结果输出光束 139 是携带指纹模式 p′的信息光束。带有空间指纹信息的光束 139 进入到相关器 142 并且通过傅里叶变换透镜 143。存储在卡 20 上的滤波器信息 F 由读卡器 72 读出并输入到处理器 80。该处理器把输入的数字滤波信息信号转换成模拟 SLM 驱动电压。这些代表滤波信息的驱动电压传送到线路 79 上的 SLM144 里。写在 SLM144 上的滤波器通过一种光相关操作中的一部分的乘法方法调制指纹的光变换，该操作把用户的指纹和存储作在用户的卡上的编码滤波 F 所代表的指纹进行比较。SLM144 的输出是一个光信号 S′，S′与变换函数 S 的相似性取决于输入指纹 P′和用来构造滤波 F 的基准指纹 P 之间的相关度。如果 P 和 P′是相同的指纹则 S′等于 S。含有 S′的光信号 145 通过第二变换透镜 146 并进入到检测其强度以分布 S′的光检测器 148。当 P′等于 P 时，S′将是表示数字数组 g 的强度分布，这些数字数组代表着唯一数 u。光检测器

148 的输出输入到处理器 80，后者从数字数组{g_1，… g_n}计算唯一数 u．如果检测器 148 的检测误差仅允许从 0 到包括 m-1 在内之间的β 个不同值，其中 m 是光检测器 148 的动态范围，我们计算:

$$g_i^*=g_i(\text{测量值}).\frac{\beta}{m}$$ 然后舍入成整数

其中 $0\le g_i^*<\beta$

则

$$u=g_1^*\beta^{n-1}+g_2^*\beta^{n-2}+\cdots g_n^*\beta^0$$

接着把数 u 作为种数输入到伪随机数发生器 84．重要的是要注意到只要向伪随机数发生器输入相同的种数（在本情况下为 u ）它都生成相同的随机数．由伪随机数发生器 84 导出的随机数以及在线路 82 上的 u 都输入到密钥生成器 88．该密钥生成器利用已知的公共密钥密码技术从这些输入推导出一个专用密钥或者一个公共密钥．通过按下辅助键盘 74 的按钮 76 促使密钥生成器在线路 90 上把公共密钥输出到公共密钥通信机 94．通信机 94 可化简单地是一个显示器或者是一个例如调制解调器的传送机，其把该数传送给发送器。

如果用户具有一个他想解密的加密报文，他可以按如下利用设备 70 对它解密．把加密报文输入到输入报文存储器 98 里。然后用户（接收者）把他的卡 20 插入到读卡器 72 里，按下辅助键盘 74 的按钮 79，并且把他的手指按在输入屏 128 上。和前面一样，处理器 80 从强度分布 S′生成唯一数 u，并且该数 u 和由随机数发生器 84 响应种数 u 生成的随机数一起输入到密钥生成器 88．响应按钮 79 的促动，密钥生成器利用这些输入推导出专用密钥．接着在线路 92 上把专用密钥输入到解密/加密系统 96；存储在输入报文存储器 98 里的加密报文也输入进系统 96．系统 96 利用已知的公共密钥密码技术从这些输入中对该报文解密．然后解密后的报文输出到可由用户访问的输出报文存储器 100 里。

如果使用设备 70 的人其指纹不是由编码滤波 F 所代表的指纹的那个人，则由卡的滤波 F 和该人指纹的傅里叶变换 P′相乘所导出的光信号 S′不等于 S．这意味着从 S′间接导出的唯一数 u′将不等于 u．所以由专用/公共密钥生成器 88 生成的密钥将不能解密加密的报文。

按下述方式利用设备 70 一个人可向一个用户发送加密报文。这个人

把明码文本报文存储到输入报文存储器 98 里，按下操作员输入设备 74 的按钮 77 并且向公共密钥接收器 95 输入该用户的公共密钥。这促使密钥生成器 88 直接从公共密钥接收器 95 向解密/加密系统 96 输入公共密钥。系统 96 使用该密钥加密明码文本报文并且把加密报文输出到输出报文存储器 100 。然后该人可以向该用户以任何不安全的方式发送加密报文。(可以注意到当按按钮 77 时设备 70 的指纹及读卡子设备是无用的。)

很明显本发明的系统允许用户在不知道他的专用密钥的情况下使用公共密钥密码技术。这增强了系统的安全性。此外进而第三方不能使用丢失的卡，因为只有通过输入用户的指纹才能恢复唯一数 u 。

本发明的另一个优点在于用户不需要知道他的公共密钥，因为借助本发明的系统可以方便地生成该公共密钥。另外，如果一个非授权个人强入到图 2 的设备 70，他没有方法确定生成 u 的方式，图为该数只在图 1 的登记设备里生成并且对于每个人它是唯一的。

本发明的系统的鲁棒性可以按下述增强。在图 1 的登记设备 10 里 $g=\{g_1, \cdots g_n\}$的一个点例如 g_1 的绝对值可以存储在卡 20 上。如果这样做，图 2 的处理器 80 以后可以把由光相关器 142 生成的 g 函数的该相同点的强度和存储在卡上的该点的强度进行比较并且相应地调整相关器 142 生成的 g 的各个元素的值。这将减小设备 70 中出现的”噪声“的影响。例如，输入屏 128 上的灰尘和油渍会减小 g 的绝对强度。但是，应该保留δ函数的相对强度。接着通过把由相关器 142 生成的 g 的一个点和以绝对值形式存储在卡 20 的 g 的相同点进行比较可恢复绝对值。

在本发明的另一种实施方式中，唯一数 u 和相关器输出的峰值位置有关，而不和迄今为止所考虑的它们的相对强度有关。在这种实施方式中滤波器 F 设计成在相关平面检测器上产生一系列等强度的峰值。仔细地控制峰值位置，从而这些峰值出现在检测器上的 p × g 个单元的网格内。当相继显示 n 个这种序列的峰值时，只利用峰值位置信息就可重现唯一数 u .

在该实施方式中一个人将采用下述程序登记。参照图 1，该人将把手指（们）按在输入屏 28 . 如前面所描述，指纹信息输入到 ICDD41 . ICDD 的数字输出 42 输入到唯一滤波器生成器 43 以及唯一数发生器

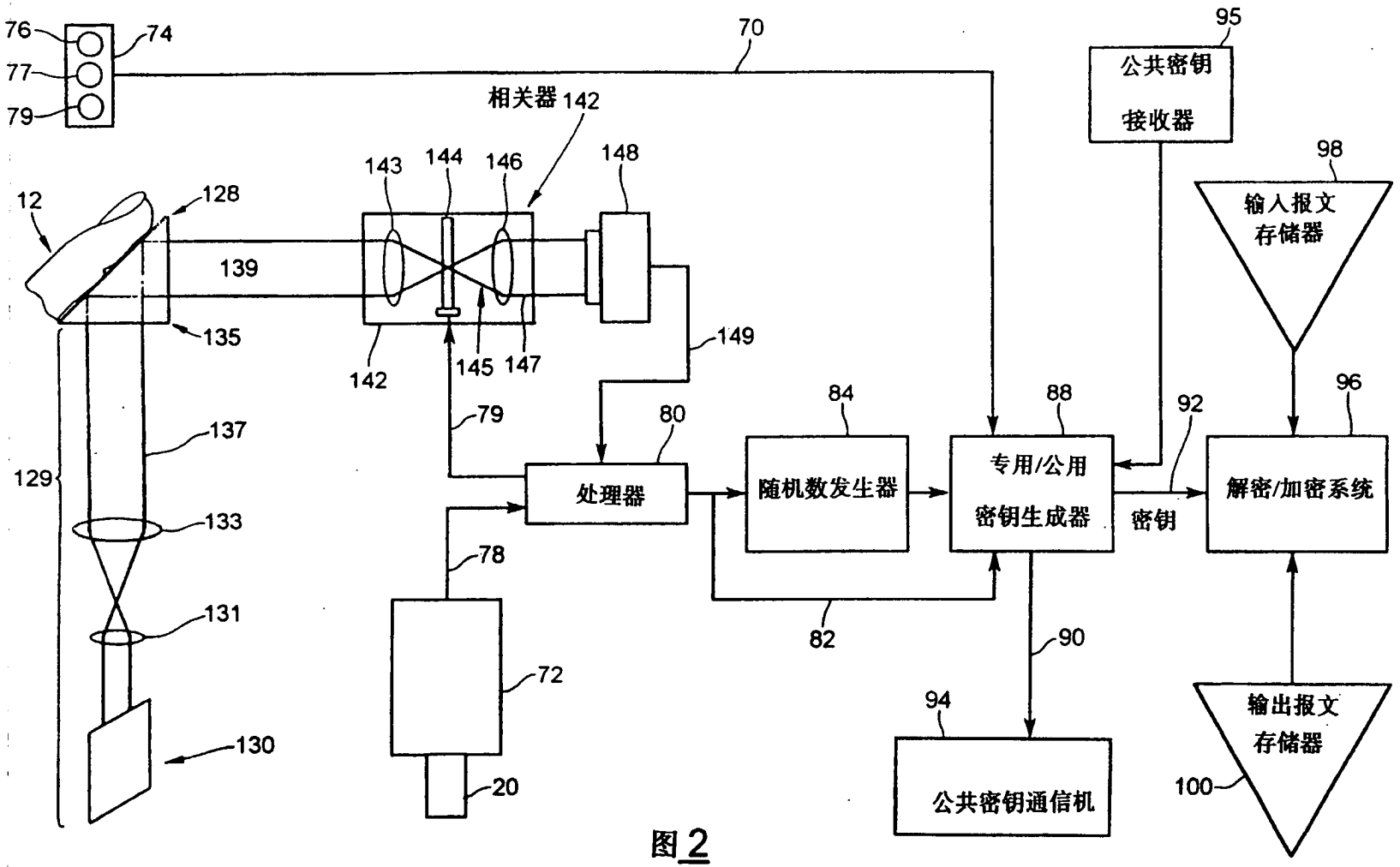

76
74
77
79
70
95
公共密钥
接收器
相关器 142
143
144
146
148
98
输入报文
存储器
12
128
139
135
142
145
147
149
96
137
129
79
80
84
88
92
处理器
随机数发生器
专用/公用
密钥生成器
密钥
解密/加密系统
133
78
131
82
90
72
94
130
20
公共密钥通信机
输出报文
存储器
100

图2